NIST SMART GRID ADVISORY COMMITTEE (SGAC) MINUTES OF AUGUST 17-18, 2017, MEETING NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY GAITHERSBURG, MD

ATTENDANCE

NIST Smart Grid Advisory Committee Members
Centolella, Paul (Chair)
Cosgriff, Kevin
Fine, James
Gracio, Deborah K.
Grijalva, Santiago
Handley, Jason P.
Holland, Michael J.
Joseph, Janet
Lee, Audrey
McDonald, John D.
Sanders, Heather

NIST Staff
Anand, Dhananjay (DJ)
Burns, Martin
Bushby, Steve
Chin, Joannie
Eustis, Allan
FitzPatrick, Jerry
Gopstein, Avi
Greer, Chris
Griffor, Edward
Harary, Howard
Hastings, Nelson
Hefner, Allen
Holmberg, David
Kandaswamy, Anand
Kneifel, Joshua
Li-Baboud, Ya-Shian
Nguyen, Cuong
O'Fallon, Cheyney M.
Song, Eugene
Wollman, David

Others
Allan, Sharon, Smart Electric Power Association
Friedman, Sara, Government Computer News
Hargrove, John, Sam Houston Electric Cooperative Inc.
Johnson, Eric, Department of Commerce
Krayem, Norman, Holland & Knight
Le, Vincent, Federal Energy Regulatory Commission

Wedin, Randy, Wedin Communications
Villarreal, Chris, Plugged in Strategies

Summary of Key Themes and Strategic Guidance Received from the Committee.

A number of key themes emerged from Committee member comments over the course of the meeting. These included:

- The electrical system—from architectures to economics to operations—is changing dramatically, and the NIST Interoperability Framework should be updated to reflect this.
- The interaction of the smart grid with larger systems, from cities to the environment, is important. Elucidating the linkages between and reliance upon existing infrastructures is crucial.
- Questions persist about how to measure cybersecurity in the smart grid, and how multiple systems interacting together can induce unintended points of vulnerability.
- The historical concept of system and device control within the electric sector needs to be updated. Where the intelligence and control resides in the system will have major implications on supporting infrastructure, value propositions, and risks, all of which need to be better understood and measured.
- As intelligence is pushed to the grid edge, understanding the dimensions of grid security and how best to achieve desired levels of protection is becoming more complex and dynamic, requiring ongoing attention and additional research.
- No single grid architecture, model, or decomposition is adequate to describe the grid, its operations, or its value.
- As data is produced in ever greater amounts and system intelligence is pushed outward, a number of issues must be addressed from data quality to data access.
- NIST outreach is important to inform stakeholder planning and other processes across sectors.
- With the expansive scope of smart grid issues, the Committee urged NIST to prioritize its engagement so that the program's limited resources are maximized by focusing on high-impact areas for which NIST is essential.

The notes which follow provide a fuller context for the emergence of these themes through the course of discussion. Unless specifically noted, these minutes reflect the comments and contributions of Committee members.

Day 1 -- August 17, 2017

Call to Order – *Dr. Chris Greer, Director, Smart Grid and Cyber-Physical Systems Program Office*

Dr. Chris Greer called the meeting to order at 8:30 a.m.

Opening Remarks and Introductions – Mr. Paul Centolella, Chair, Smart Grid Advisory Committee

Mr. Centolella introduced himself with a brief bio related to smart grid activities, and then the Committee members each similarly introduced themselves. Mr. Centolella highlighted the important role the committee plays as part of the overall NIST mission. In keeping with NIST's reputation for outstanding science, he encouraged the committee to bring its best effort over the next two days, to ask many questions, and to look for ways in which the smart grid program can be enhanced.

NIST and Engineering Laboratory Update – *Dr. Howard Harary, Director, Engineering Laboratory*

Presentation Summary – Dr. Harary provided an update, including an overview of NIST's mission,

organizational structure, programs, and services. He provided a detailed discussion on the Engineering Laboratory's mission, structure, and goals, as well as its set of unique facilities and engineered systems research programs. See slides of Dr. Harary's presentation.

Smart Grid and Cyber-Physical Systems Program Overview – *Dr. Chris Greer, Director, Smart Grid and Cyber-Physical Systems Program Office*

Dr. Greer provided an overview of the Smart Grid and Cyber-Physical Systems (CPS) Program, including details about the FY17 budget, core personnel, and program strategy. Providing a closer look at the CPS program, he discussed examples of activities in three key areas: foundations (CPS Framework), experiment/testbed (Universal CPS Environment for Federation), and applications (Global City Teams Challenge (GCTC), IoT-Enabled Smart City Framework). See slides of Dr. Greer's presentation.

The Committee and Dr. Greer had an extended discussion about smart cities. Smart grid is at the heart of smart city applications. Smart grid is a component of smart cities, and they share larger societal goals (e.g., resilience, sustainability, productivity.) An important issue for both smart grid and smart cities is valuing and measuring what the grid does to support cities and communities. For example, how can we measure the value of resiliency or the value of various grid services? Measurements such as Key Performance Indicators (KPIs) and Return on Investment (ROI) can be useful in at least two ways—helping balance competing interests between smart grids and smart cities; and helping build a case for capital investments from the private sector, the public sector, and public utility commissions. NIST is approaching the challenging issue of measuring value in smart cities from both a practical perspective (e.g., through case studies, including the business models and results of GCTC action clusters) and a theoretical perspective.

Before deploying new technology in smart grid and/or smart cities, manufacturers need a strong business case that articulates the value proposition for different stakeholders. The deployment of new technologies must also be preceded by the establishment of solid infrastructures for both information technologies (IT) and operational technologies (OT). ("We need to have a 'strong grid' before we have a 'smart grid.'") The IoT-based Smart City Framework (IES-City Framework) defines a three-step approach to analyzing smart city applications, with the second step using maturity indicators to help cities answer the question of whether their infrastructure is ready. By identifying pivotal points of interoperability and introducing metrics, it is hoped that greater understanding, more rationality, and deeper insights can be introduced into the decision-making process for cities, PUCs, and industry.

The Committee and Dr. Greer also discussed cybersecurity for smart city applications—how it can be measured and how multiple systems interacting together can introduce unintended points of vulnerability, as well as emerging behaviors. In response to the need for greater emphasis on cybersecurity in smart city applications, NIST and the Department of Homeland Security will be announcing a joint initiative, "Smart and Secure Cities," later this month at the GCTC Expo. The initiative will help explore the value propositions and ROIs related to building-in cybersecurity for smart city applications.

Smart Grid Program Overview – *Mr. Avi Gopstein, Program Manager, Smart Grid and Cyber-Physical Systems Program Office*

Mr. Gopstein provided an overview of the Smart Grid Program, discussing the Smart Grid Program's EISA mandate, program strategy, and budget. He discussed examples of activities in three key strategic areas: foundations (Smart Grid Framework), experiment/testbed (Smart Grid Testbed, smart grid research), and applications (Transactive Energy Challenge, smart grid standards coordination). He defined a common goal and theme among the research projects: "Maximize the ability of grid systems to accommodate Distributed Energy Resources (DER)." See slides of Mr. Gopstein's presentation.

The Committee and Mr. Gopstein had an extended discussion related to the word "control," as in when speaking

about "to control distributed energy resources (DERs)." Because the electric industry has certain historical ideas about what "control" means, it was suggested that the words "coordination" or "control theory" might be better. With emerging technologies, including power electronics and microgrids, we may see a very different approach toward managing disruptions in the grid, including islanding and coordinating with neighbors. This new approach (i.e., coordination or control theory) will also involve markets, including localized markets, as well as intelligent devices. The coordination may take place in a manner that combines centralized dispatch of larger resources (as with today's ISOs), localized markets, intelligent devices, and fast-acting distributed controls. In a system of systems, it is essential to consider and understand the coordination of different things operating on different levels. Through its Smart Grid Interoperability Testbed, NIST will be heavily involved in exploring the implications of coordination at the distribution level of key new technologies, including power electronics and microgrids.

The Committee also discussed the scope and breadth of NIST's smart grid research program. Several Committee members felt that a clearer strategy and more prioritization of efforts is necessary. The smart grid area is large, so it will not be possible to cover the entire system with the small budget that NIST has. How will choices be made for the smart grid program? How will NIST use its leverage? How will NIST partner with other federal laboratories, with industry associations, and with the academic community? Mr. Gopstein replied that the Framework process, to be discussed later in the meeting, will provide a key opportunity for NIST to develop and describe its strategy. One Committee member said that they were shocked at the enormity of the program's goals as compared to the magnitude of the budget. ("Are there zeroes missing?") They were concerned that this budget mismatch is emblematic of how we as a society are underestimating the enormity of the challenge in this grid modernization transition. NIST must prioritize and focus on high-impact areas—those areas for which NIST is essential.

A Committee member said that a safety architecture on top of all of this will be important, just as a cybersecurity architecture needs to be on top of all of this. For example, what happens when inverters aren't functioning properly? Mr. Gopstein agreed that safety is important, and that it falls under the term "trustworthiness," where the focus is on the operations of the overall system rather than the protection of one aspect of it.

Committee members identified some key research areas for NIST to consider, including the following:

- stability (e.g., how many inverters can be added in a region?)
- the need for a coordination framework for industry (e.g., how will distributed optimization work?)
- monitoring, control, and coordination (e.g., how do we optimize across multiple, interconnecting microgrids?)
- what information should be brought from the microgrid level to the Advanced Distribution Management System (ADMS) level (and vice versa)
- the integration of devices and the aggregate impacts
- distribution system dynamics (including synchrophasors at the distribution level and power electronics)
- architectures (including safety and cybersecurity architectures)
- end-to-end testing to ensure interoperability
- doing value analyses in all areas (e.g., value to utilities, value to end-use customers, etc.)

A Committee member concluded by encouraging Committee members to continue examining what NIST—with its unique leveraging ability to highlight gaps and to convene stakeholders—can and should do.

Ethics Briefing – *Mr. Eric Johnson, Attorney, Department of Commerce*

Mr. Johnson provided an ethics briefing to Committee members.

Smart Grid Interoperability and Building to Grid Integration – *Mr. Steve Bushby, Group Leader, Embedded Intelligence in Buildings Program*

Mr. Bushby presented an overview of the Facility Smart Grid Information Model (FSGIM), an example of a completed project in the smart grid program. FSGIM, which is now a national and international standard, was developed to address problems related to energy management in the building sector. NIST's leadership on this project is an example of NIST's capabilities, including technical leadership and the ability to bring together diverse stakeholders and standards development organizations (SDOs). See slides of Mr. Bushby's presentation.

A Committee member asked how the FSGIM standard deals with various emerging issues, including the following:

- energy providers and building managers interfacing with many different energy management systems
- breaking down loads in building (including using machine learning techniques to understand waveforms)
- taking advantage of knowledge and modeling about a building's thermal characteristics (such as inertia) to improve optimization

Mr. Bushby replied that FSGIM is an abstract model. It is not a communication protocol, but it describes the type of information needed. It is a stepping stone towards solutions, not a solution in itself. In the commercial building space, it can help define ways to represent complexity, map performance, and make decisions.

When asked his perspective on the issue of open source vs. proprietary building energy management platforms, Mr. Bushby replied that the "open source vs. proprietary" question is not the most important issue. Building energy controls haven't made a bigger impact in this sector because of business barriers, not technological barriers.

This session concluded with an observation that better integration of buildings is an important issue and some questions for future discussion. How do we get more building energy management systems actually working in the field? How can we help building managers better understand the potential benefits? What are the barriers to doing this communication? Is there a role for NIST in this effort?

Smart Grid Cybersecurity – *Dr. Nelson Hastings, Group Leader, Cybersecurity and Privacy Applications Group*

Dr. Hastings presented an overview of work related to the security of grid edge devices, an example of a current research project in the smart grid program. A key goal is to develop a strategy for decomposing system-level cybersecurity guidelines (found in NISTIR 7628, "Guidelines for Smart Grid Cyber Security") so that they can be applied to grid edge devices. Profiling the performance impact of security solutions on grid edge devices, and exploring how to secure publish-subscribe communications—a project done in conjunction with the SEPA OpenFMB Cybersecurity Task Force—are two ways NIST is working on this issue. See slides on Dr. Hastings' presentation.

The Committee discussed tradeoffs that must be considered as we consider cybersecurity issues. Many manufacturers think that that we can add cybersecurity functionality to a device or system without affecting performance. However, there are likely to be performance impacts on overhead and the memory that's needed. At which level(s) of a system architecture will we want to use cybersecurity? What is the value vs. cost tradeoff of what you're protecting? What is critical and what isn't? How can we tell if it is "secure enough"? How much cyber is needed to make it a "secure system" instead of just a "secure device"?

The group discussed how different architectures can affect cybersecurity. For example, security is being pushed to

the edge today because decisions must be made faster, and that can't happen in a centralized fashion. Another example is the increasing role of aggregators, who are adding an additional layer of devices and complexity as they install gateways at the house. Architecture is extremely important, but it will not simply be either distributed or centralized, but rather it will be a hybrid of the two. One utility is looking at four approaches—centralized, substation, nodal, and premises.

We need to determine what cyber functionality is required at each level of the architecture (substation, premise, device, etc.), as well as at the entire system level. What level of cybersecurity is needed by whom for which use case? We can't put every cyber functionality into devices with low processing and memory capabilities. At the higher levels in the architecture, we can start "white-listing" devices, but that is impractical for distributed systems.

NIST's first step in looking at some of these cybersecurity issues is to look at edge devices. Eventually, NIST would like to approach this by looking at three different architectures—edge grid, medium commercial (e.g., aggregated solar at a larger scale), and utility-owned asset inside a substation with a gateway.

We shouldn't just assume that the addition of cybersecurity will have a negative impact on performance. As we add secure smart devices and appliances to the ecosystem, it may also open up new opportunities and innovations that bring new economic benefits. For example, by collaborating with manufacturers, there may be opportunities to optimize existing code and design to eliminate the added latency that can come with increased cyber functionality. As another example, already-deployed smart meters have capabilities that haven't been turned on yet. What is the difference between what devices could do in the future, and what they're currently being asked to do? What are the economics of why we aren't turning on these capabilities?

Committee members made some specific recommendations related to cybersecurity, including the following:

- In its cybersecurity testing, NIST should consider key edge devices such as relays and not just behind-the-meter technologies such as EV chargers or thermostats.
- NIST should become familiar with the IEEE 1686 standard, which is a standard for intelligent electronic devices' cybersecurity capabilities at the device level.
- When testing how a specific cyber functionality affects device performance, it's important to also consider the latency of communications across the system.
- NIST should think about commoditizing cybersecurity in terms of the device's purpose and to consider the risk framework around a device. If a device is compromised, how is the overall system affected?

The discussion concluded with observations directed to NIST in general. It is important to think more laterally and not just within only the scope of smart grid. As seen in some recent cyber attacks, other loads and devices, in aggregate, can be operated maliciously and that could have an effect on the grid.

Grid Architecture and System Dynamics – *Dr. Dhananjay (DJ) Anand, Researcher, Smart Grid Program Office*

Dr. Anand described a potential research project, "mitigating the impact of stochasticity in future power systems." This is an example of a future research project in the smart grid program. He discussed sources of uncertainty and variability in distribution circuits, and he reviewed various approaches (e.g., improved measurements, better modeling and validation, etc.) for reducing and understanding "epistemic uncertainty" and "aleatory variability." He proposed a methodology involving three concurrent strategies. Validation will involve using a distribution circuit on the NIST campus (which already includes photovoltaics), adding sensors and smart meters, and then using the testbed to validate modeled behaviors. See slides on Dr. Anand's presentation.

A Committee member commented that these are risky projects. He suggested that working with a very small system (e.g., IEEE 13 bus system) might be a good first step. Other labs looking at projects related to the topics of

integration and stochasticity are NREL, Sandia, and PNNL. This Committee member said that a project that would be very helpful to industry would look at the following question: If you have a model of the system and the measurements for that system (coming from real-time SCADA, smart meters, and PMUs), how do you tell how good your model is?

Another Committee member asked whether there is a machine learning aspect to using weather data to get forecasts? Dr. Anand said our first steps have just involved aligning the features from satellite data and what we see from the ground.

A third Committee member raised the issue of individual sources of uncertainty that are then aggregated in a portfolio, such as on the grid. Do you exacerbate or mitigate uncertainty? Is there a possibility of compensating error?

The discussion concluded with a comment from a further member of the Committee that there is value in focusing on both the issue of variability and the issue of measurement uncertainty (and trying to minimize each of them).

SEPA Update – *Sharon Allan, Chief Innovation Officer, Smart Electric Power Association (SEPA)*

Ms. Allan provided an update on the activities of the Smart Electric Power Alliance (SEPA). She reviewed the history of the Smart Grid Interoperability Panel (SGIP), which merged with SEPA earlier this year. She reviewed organizational accomplishments so far in 2017, including numerous webinars, progress with priority action plans (PAPs), as well as recent additions to the Catalog of Standards. She provided an overview of the mission, membership, staffing, budget, and governance of SEPA, and discussed some of the highlights from the Grid Evolution Summit held in July. SEPA's focus for 2017 is to complete the integration of the two organizations. Speaking on behalf of SEPA, she said that SEPA appreciates the opportunity to work with NIST and looks forward to continuing our efforts together. See slides on Ms. Allan's presentation.

Discussion of Plans for NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0 – *All*

Mr. Gopstein presented a brief description of the NIST Framework in order to set the stage for the committee's general discussion. The Energy Independence and Security Act calls for NIST to "coordinate the development of a framework" for smart grid interoperability. The Framework document has evolved over its first three versions, which were published in 2010, 2012, and 2014. The electricity sector and smart grid have changed very significantly in the past three years. He invited the committee's discussion and feedback as NIST embarks on a major revision of the Framework over the next year. See slides on Mr. Gopstein's presentation.

The Committee then held an open discussion, with many topics discussed and perspectives presented. For the purpose of these Minutes, the Committee members' comments have been grouped into general themes.

Domains -- The group discussed the NIST conceptual model and how it might need to be changed in Framework V4. Suggestions for new domains included Environment; Transportation and Electric Vehicles; and Smart Cities. It was noted that the European Union treats renewable energy and storage as a separate domain. From state to state in the U.S., there are wide variations in how different domains interact.

Within existing domains, there have been important changes in the past three years:

- Consumer domain
    - In the "prosumer" model, the customer is both a producer and a consumer. What are the implications for measurement and interoperability?
- Service provider domain
    - Business models for energy services have become more diverse (e.g., aggregation, microgrids).

- Storage
    - Storage is currently shown in three domains. See further discussion on storage below.
- Interfaces between domains (e.g, transmission/distribution or distribution/customer)
    - Many changes, innovations, and transformations are taking place at these interfaces.
- Distribution
    - With increasing Distributed Energy Resources, efforts to identify the value of these resources with greater temporal and spatial granularity.
    - The changing function of Distribution System Operators and development of Distribution System Platform concepts (including transactional and services platform concepts).

Architecture -- Instead of just one architecture, there will be a number of different architectures. The number of viable architectures is expanding, and no single model is adequate. As architectures are changed, there will be impacts on operations, economics, cybersecurity, and testing and certification.

There is a need for an architecture that represents a low-carbon future. A low-carbon future would involve replacing much of our existing generation mix (or capturing the carbon from it). It would also involve electrifying many of our end uses, and this may increase electricity requirements by a factor of two.

Architecture issues are being discussed by countries around the world. Are there elements from these other architectures that we could incorporate into our architecture possibilities?

Architecture is more than just a laminar decomposition (as was depicted in NIST Framework 3). We also need to decompose it in terms of location, time, power, reactive power.

Other "architectures" were discussed, including architectures for cybersecurity, innovation, platforms, industry, markets, communication, and coordination.

Other "architectures" were discussed, including architectures for cybersecurity, innovation, platform business models, industry, power markets, cross-sectoral (gas/electric and electric/transportation) markets, communication, and coordination.

Data, Analytics, and Embedded Intelligence -- The amount of data—and its granularity (for both space and time)—is rapidly increasing, raising a number of issues. These include custody, allowable uses, control, transparency, integrity, security, and privacy. It was suggested that rather than talk in terms of ownership, a better question is: Who has what rights to use which data under what conditions for which purposes? At the macro level, who gets to analyze the data and for what purpose? Who can derive value from the data? Who has a stewardship responsibility to use data to create value and under what conditions? How does data serve the issue of interoperability?

In the last few years, there has been a big increase in use of embedded intelligence in devices, such as smart sensors. Processing and memory capabilities are going up as price is coming down. More of the analytics can now take place at the edge, rather than at a central location. Can we get additional data from deployed smart meters? How good is the data and what can it be used for? What will be the future of smart meters as additional sensors are embedded in devices and deployed?

The Committee also discussed the security of grid data and the quality and security of data from internet connected devices.

Storage -- In Framework V3, storage is shown in three different domains. The issue of storage has changed very significantly since Framework V3 was written four years ago. Storage can be used for many purposes, and it can provide more than 40 different services.

Storage is not well understood by many regulators. NIST could play a role in educating regulators about storage and encourage them to think about storage in new ways (not just in the boxes to which it is assigned now).

For energy storage, from a business standpoint, it's important to understand valuation, monetization, and measurement. If storage plays into four different markets at once, interoperability is an important consideration (and a topic where NIST can make an important impact).

While storage costs are coming down, storage is commercial grade but not yet utility grade. We aren't ready yet for "set-and-forget" batteries at utility-scale storage facilities, because auxiliary power loading and cooling require constant attention. In the future (five years out), we must dramatically improve the reliability of storage, and it must become "low-touch."

Regulation and Education -- For many of the issues the committee has discussed, regulation is a bigger barrier than technology. Regulation plays a very important role in making it possible to incorporate these new technologies, architectures, and business models. NIST can play an important role in educating regulators.

NIST can also play a role in educating industry about standards and about the difference between conformance/compliance and interoperability. For example, if you are a utility or a vendor, which standards do you need to take into account? What are the foundational standards?

When utilities adopt new technology, you need to adapt business processes, change organizational structure, and employ new skill sets. A report from Price Waterhouse Cooper report said that 40% of energy industry employees and 60% of energy executives will retire in five years. How does this affect the Framework?

First Day Wrap-up – *Dr. Chris Greer, Director, Smart Grid and Cyber-Physical Systems Program Office*

As the preparation for the next day's discussion, Dr. Greer encouraged members to think about two questions:

- What has changed significantly since 2013?
- What are the problems that NIST should be trying to solve?

Day 2 -- August 18, 2017

Smart Grid Interoperability Testbed Tour – *All*

The Committee received a tour of the Smart Grid Interoperability Tour, including presentations by NIST testbed researchers (Dr. Allen Hefner).

Discussion on NIST Smart Grid Research Portfolio and Future Priorities – *All*

For this discussion period, Mr. Centolella posed a series of four questions to Committee members.

How have things changed since 2013?

Here is a list compiled from Committee members' comments:

- Increased volatility due to high penetration of renewables on the distribution network
- Less inertia and less spinning reserve in the system as more DERs come online
- Loss of base load
- Mechanical means of control don't make sense any more
- Embedded measurement and sensing are increasing
- Synchrophasors are being increasingly used at distribution level
- Increased use of power electronics
- Increased use of grid edge controllers
- Increased use of power electronics controllers (e.g., low-voltage dynamic grid-edge controllers)
- Distributed intelligence and edge computing capabilities have increased
- Increased capacity for analytics at the edge (edge grid control and analytics).

- Interface between transmission and distribution domain is changing
- Operational inter-dependence is getting more complex (e.g., what happens when sun sets in CA?)
- More microgrids
- Falling costs of DER
- Storage costs are coming down; new use cases for storage
- New models for DER (virtual power plants, non-wire alternatives)
- Utilities are "refreshing" their AMI deployments (second round of smart meters)
- Expectations for spatial and temporal granularity of data have increased
- Prosumer model introduces additional roles for the consumer
- Platform models are being explored, discussed, implemented (e.g., NY REV)
- Highly electrified, low-carbon future is becoming more likely (e.g., in New York City)
- Goal of grid adversaries has changed, and the new goal is to bring down the grid

What is the objective of the Smart Grid Program? What is the problem we are trying to solve?

The objective is to create net value to society and the users of the grid through the operation of the grid. "Net value" includes resilience, reliability, efficiency, optimization, integration, security, and safety. Current business models for utilities need to be changed in order to accomplish this goal.

NIST objective should be "plug and play." What it will take to achieve that? What is the path to get there?

We now have a much quicker innovation cycle for technology. Time frames for utilities and digital technology organizations are different. Utilities are used to 30-year asset lifetimes, but they are now talking about moving to 15-year asset lifetimes for metering, 10-year lifetimes for digital assets, and 5-year lifetimes for communication equipment. NIST can help propagate this new approach to regulators. How do we match a 5- to 10-year standards development timeline with a much faster innovation cycle? NIST can help compress this time.

How can the grid be "future-proofed"? When a utility buys equipment today, how can it best protect that investment?

NIST can help set expectations and give guidance to policy makers about standards, compliance, and interoperability, and about what is necessary for technology adoption. We need better ways to communicate with policy makers (not just reports), because attention spans are short.

The EISA mandate for NIST is broad and gives NIST considerable flexibility. NIST can use the Framework to define a future state. NIST should be bold with this Framework.

What are important changes (e.g., related to standards, research, working with others, etc.) are anticipated that NIST should prepare to address in next five years?

Here is a list compiled from Committee members' comments:

- Need for more flexible, dynamic load and everything that's associated with it, including measuring it, controlling it, and monetizing it
- Dealing with greater penetrations of distributed energy resources (DERs)
- Increased use of big data to be more precise in how we operate the grid and reward assets on the grid – at lower cost. What are you going to use it for and how much value does it add? This is a big issue in terms of interoperability, distribution of data, and use of data. How does data serve the issue of interoperability?
- Increased use of data analytics to improve asset management.
- Increased computing capability at the grid edge and associated issues (distributed analytics). NIST has the opportunity to start bringing clarity to the issues that need to be tackled in this area. Industry will be investing lots of money, so we should help them avoid mistakes.
- Need for better simulation and modeling, including dynamic modeling (e.g., how to model multidirectional power flows in a distribution system with advanced distributed energy resources (DERs))

- The way we communicate between devices will be changing to "publish and subscribe" (instead of today's hub-and-spoke or star methods).
- Need to improve reliability of storage for utility use (storage must be almost "set and forget")
- We will need more use of DC, including providing DC service.
- With decentralization and more distributed aspects in the future, is this going to be a net strength or weakness for the grid in terms of cybersecurity. Can NIST help tease out answers to this question through its testbed?
- Customers, vendors, and utilities are moving to cloud-based platforms, including for operations and customer data. What are the implications for security?
- In the future, data management and applications may move to distributed ledgers or blockchains. What new standards will be needed?
- The information and communication industry will continue to innovate at a faster rate than the utility industry. Which new technologies (e.g., blockchain, fog computing) will be most useful for the smart grid?
- Increasing use of dynamic models (e.g. incorporation of dynamic line ratings into grid operations) to improve asset utilization and responsive devices and respond to price signals or grid conditions.
- Increased electrification (more electric vehicles, greater penetration of heat pumps and electrification of heating, more computers and associated cooling) and greater capacity will be needed for the electric system.
- Distributed market model in the distribution system (including locational marginal pricing and options contracts that allow utilities to dispatch specific resources)
- More prosumers
- The regulation model needs to help move things forward, encourage the creation of value, and enable utilities and/or third parties to create value. If NIST were to have a role in this area, it could involve providing input into "regulatory school" for PUC staff and new commissioners.
- NIST should provide education/outreach to regulators, industry, and consumers. In doing so, NIST should including more real-life examples and deliver messages more effectively.

Here are two general statements offered by Committee members that sum up many of the comments listed above:

- We need a model that knows the right way to integrate the continued, necessary, centralized dispatch of big generators on the bulk power system with:
    - the operation of many more DERs
    - power electronics
    - new technologies for distributed computation, analytics, and control, and
    - the operation of distributed marketplaces.
- To be fully interoperable, the grid must have interoperability at and across many levels—the physical equipment level, the control level, the communication level, the overall system control and coordination level, and the market and business level.

Dr. Greer posed this closing question to the committee: Given this potentially large scope, the quadrant we chose is the distribution grid. We didn't choose transmission or interconnects between those. We also chose to focus on accommodating and optimizing DERs on the distribution grid—and all that goes with that (e.g., new control paradigms, distributed intelligence, new actors, new regulatory environments). These are our initial choices. Have we made a good choice?

The answer from one committee member was, "You made the right choice. The distribution arena is the right place to focus right now."

<u>Where are the NIST-specific opportunities to leverage and execute?</u>

A Committee member asked the following general question: If we agree where we need to be in five years (e.g., flexible and controllable dynamic loads), has NIST done an analysis to see what is needed to make it happen, where are the interoperability gaps and needs for standards, and who needs to contribute?

Dr. Greer answered that member had just provided "an eloquent description of our Framework process." Frameworks V2 and V3 were incremental. Framework V4 must be wholesale change. We are just entering into that process.

NIST's role under EISA is to coordinate standards, not to write them. NIST established SGIP as the way to focus on gaps, form priority action plans, and find the right people and organizations to work on them. That's what SGIP has been doing for the last several years.

NIST is encouraged to use the Framework consultation process for the issue of distributed analytics. Bring the communities together and learn what kind of analytics will add more value over the longer term, what kind of analytics are possible. Then work toward an interoperability framework that can help those vendors that are building edge devices and analytics. What are the interoperability standards that could help them build devices to a standard that will help the smart grid, consumers, etc.?

In developing a new framework, NIST should consider approaches for "building in" security from the beginning. We need verification techniques already built into the analytics so that you know the data and analytic output are valid. Perhaps we need a certification model for these applications.

As we look at these areas, it may affect who should be on this committee. Maybe we need to get people from outside "our family," such as regulators or technology industry leaders. (Comment from Dr. Greer: This committee has the ability to create subcommittees where it might need and want input from others.)

Mr. Centolella invited general reactions and comments from NIST staff.

- Mr. Gopstein said that the concepts described (i.e., decentralization of control, communications, and analytics) are concepts that we've been trying to incorporate. It matches very well with our research program and integrated testbed. Over the past two days, the committee has expressed these ideas very articulately, thereby validating them and giving them greater focus and prioritization. We are very grateful for this.

- Mr. Gopstein also said that, on the issue of cybersecurity concerns and constraints in the testbed, we have room to grow. Now that we have a common workspace in our testbed, we can leverage the best knowledge and people in a way we haven't been able to do before. This reinforces the importance of integrating the research streams.

- Regarding the Framework, Mr. Gopstein commented on the possible need for new domains, such as a transportation domain. Up until now we have looked at the grid as fixed, but electric vehicles introduce a new dynamic and may need to be treated in a new domain.

- Dr. Hefner discussed SGIP's Domain Expert Working Group (DEWG) on Distributed Renewables, Generation, and Storage (DRGS). This group looked closely at the multi-level control architectures needed for high penetrations of distributed energy resources (DERs), such as aggregators, demand response management systems (DERMs), and mobile DERs. Although a specific priority action plan was not created, the technical output from this group has been included in standards efforts. They also looked at power electronics integration with other discrete items on the grid (e.g., IEEE 1547).

- Dr. Wollman commented that there is a large body of work that we have done through various technical groups with SGIP and standards organizations. As mentioned by others today, we need to reframe, simplify, and elevate this technical work to make it more accessible for regulators and others.

Dr. Greer offered three summary comments on focus, context, and next steps.

- With respect to focus, his metric for an appropriate level of focus is whether we can express our strategy in a simple phrase. He offered a draft phrase: "To coordinate making 'distributed' work for distribution." ("Coordinate" refers to the EISA mandate and associated consultation processes. "Distributed" means DERs, edge devices, cloud/fog transitions, more data streams, better analytics, new actors at the edge, etc. "Work" means that it must be safe, secure, reliable, resilient, efficient, privacy-enhancing, economically viable, feasible, and consistent with regulation. "For Distribution" means that we are focusing on the distribution domain.)

- With respect to context, the smart grid program works within the cyber-physical systems program. What are basic CPS principles and how can they be applied to specific sectors? What are we learning from smart cities about how the grid interacts with other infrastructures?

- With respect to next steps and the Framework development process, this committee is helping us test drive and tune up how we will work with broader communities. We will be launching the Framework process, which will include a series of consultations. We will make the committee aware of these consultations as we are planning them, and we hope you will participate as able. We expect that the Framework process will take about 12 months to produce a good draft. In six or seven months, we will be deep into the process, but we won't have it finalized. That might be a very good point to bring this committee together again. Although we normally have only one in-person meeting and one virtual meeting each year (as specified in the committee charter), we might consider whether more meetings would be helpful during this Framework process.

Public Comments

A member of the public offered the following comments, mostly related to regulatory issues:

- Not every state is on board with the concepts and vision discussed at this committee meeting. Some commissioners wonder why a state even needs to think about distribution platforms.
- It is very helpful that this committee has members with regulatory experience. However, the individuals on this committee are not "typical regulators," so it might be useful to look beyond just California, New York, and Hawaii.
- "Prosumer" is a misnomer. The premise will be doing the work. The work is going to be automated and aggregated, so it will not be done by an individual.
- Data management questions were raised by FERC's Notice of Proposed Rulemaking (NOPR) on DER last year. FERC said that the discussions should happen at each of the ISOs. There may be a role for the NIST Framework to inform the ISO process.
- NIST may be able to contribute to the discussion of how much base load is needed. How do you operate a system with less reserves? How do you move beyond the concept of base load?
- Metrics for reliability are inadequate, especially considering the amount of data available. What are potential metrics beyond SAIDI (System Average Interruption Duration Index)?
- There has been a substantial lack of R&D investments by utilities. With respect to the important issue of testing and certification, do the utilities have enough money to create their own labs?

Planning for Next Meeting and Wrap Up – *Dr. Chris Greer, Director, Smart Grid and Cyber-Physical Systems Program Office*

Dr. Greer raised the question of when and how often the committee should meet in the coming months. The committee discussed members' willingness to help, the value of key milestones in the Framework process, and the importance of advance notice and preparation for any meetings. Regarding the possible use of subcommittees, it was noted that subcommittees report to the committee, not to NIST. The current structure for the committee

already has three subcommittees—short-term, mid-term, and long-term. Other individuals can be invited to participate on subcommittees.

Dr. Greer thanked the chairman and all committee members for a very productive meeting.

The meeting was adjourned at 12:00 p.m.